
Australia: Current Developments In Australian Army Information Operations

By James Nicholas, Major, Australian Army

Editorial Abstract: *Major Nicolas notes Australia's armed forces are considering doing away with the term "information operations" and substituting the term "information actions" in its place. IO appears to be too much of a specialist's stove pipe, as influence emanates from all military activities. This change may better reflect the relative weighting Australia places on specific aspects of information-related issues, such as the terms "decision superiority" and "influence."*

Introduction

Over a decade ago, the concept of "command and control warfare" was incorporated into US doctrine. It focused on enabling US commanders to complete their decision-making cycles more quickly and more effectively than their adversaries. Subsequently, the concept was refined and renamed "information warfare," and later replaced by the concept of information operations which has been incorporated in Australian and allied joint doctrine.

The developing concept of information operations is broader than its predecessors. While continuing to focus on the need to move through decision-making cycles more quickly and effectively than the adversary, IO also recognizes the need to influence and win support to enable friendly force military actions. This support primarily emanates from the local population in an area of operations, as well as from broader regional and international audiences.

Currently, the Australian Army is developing processes to enable conduct of information operations at the tactical level. While the Australian Defense Force (ADF) joint information operations doctrine allows the strategic whole of government to focus on operational planning, such doctrine does not provide commanders an adequate approach to conduct tactical level IO. Accordingly, many believe a gap exists in tactical Australian Army information operations.

Issues addressed here include: status of Australian joint and ABCA armies' doctrine; coalition experience; information operations versus use of the term information actions (IA); core elements of information actions; and information actions and intelligence preparation of the battlespace.

Status of Australian Joint and ABCA Armies' Doctrine

Australia published its first joint doctrine on information operations in 2002. Until early 2006 there was no change in Australian joint doctrine, and little change in the Australian/British/Canadian/American (ABCA countries') joint and armies' doctrine. In early 2006 the US issued a new US joint information operations publication. Some IO professionals envisaged that this publication, together with recent operational experience, may force change in the doctrine of ABCA armies.

Prior to 2007, the ADF produced joint information operations doctrine suited to the conduct of strategic and operational IO, but no lower order doctrine existed. The decision

to develop Australian Army land warfare doctrine (LWD) arose from the requirement to develop an Army information operations capability to address tactical requirements, for operations at brigade and below.

The 2002 doctrine provided an Australian perspective on information operations, based primarily on US doctrine of the time. Since then there have been shifts in joint US information operations doctrine, and although not fundamental, the changes are significant. In late 2006, the Australian Army finally began writing its own information operations doctrine.

Coalition Experience

Recent operational experience has generated considerable criticism of Coalition information operations. First, these criticisms include being unwieldy and difficult to apply; secondly, as being inadequate in relation to the practical aspects of gaining influence and support. This is especially significant in what may largely be an unfriendly operating environment, with an instinctively distrustful civilian population. Additionally, aspects such as training, inadequate allocation of appropriate resources, untrained staff, and inadequate intelligence support to IO, have all drawn close examination. A US commander recently wrote:

I am absolutely convinced that we must approach IO in a different way and turn it from a passive war fighting discipline to a very active one. We must learn to employ aggressive IO. We cannot leave this domain for the enemy; we must fight him on this battlefield and defeat him there just as we've proven we can on conventional battlefields.

Complicating our efforts in the information domain is the fact that we are facing an adaptive, relentless, and technologically savvy foe. Our adversary recognizes the global information network is his most effective tool for attacking what he perceives to be our center of gravity: public opinion—both domestic and international. And the truth of the matter is that our enemy is better at integrating information-based operations, primarily through mass media, than we are. In some respects we seem tied to our legacy doctrine, and less than completely resolved to cope with the benefits and challenges of information globalization.

Such feedback may have been the basis for the decision at the recent ABCA Information Operations Project Team meeting to recommend the abandonment of the concept of IO, at least in its current form. The team recommends the term 'information operations' be discarded, but that the core activity

of *influence* be retained. British Forces are also conducting a detailed analysis of the influence component of information operations.

The ABCA report recommendations were an effort to ensure a less cumbersome application of various capabilities, and to meet situations where influence and support achieve a much greater weighting than at present. Thus the Australian Army views retention of the term ‘information operations’ as non-critical; however, retention of the underlying concept of ‘influence’ is seen as paramount.

Another critical need is to remove information operations from a specialist stove-pipe, and recognize that influence emanates from all military activities: either as a planned (list order) effect, or as an unintended (second or third order) effect.

Information Operations Versus Information Actions

Apart from the ABCA Project Team’s recommendation not to retain the term information operations (yet to be formally endorsed by ABCA), further examination of how NATO sees the IO construct led the Australian Army to examine alternative terms to describe tactical level information-related actions.

One issue with the term information operations is the current variety of definitions in use. The Australian joint doctrine definition is significantly different from US joint doctrine, and those of the other ABCA services.

The varying definitions reflect the relative weighting placed by different countries or organizations on the decision superiority and influence aspects of information operations. The current US joint and Army definitions focus on achievement of decision superiority, with somewhat less emphasis on influence. The current Australian joint definition addresses both aspects. The current NATO definition reflects the need for information operations to focus on influencing target audiences. The current US, NATO and Australian Joint formal definitions are:

(US Joint) *The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own.*

(NATO) *Coordinated actions to create desired effects on the will, understanding, and capability of adversaries, potential adversaries, and other approved parties in support of overall objectives by affecting their information, information-based processes, and systems while exploiting and protecting one’s own.*

(Australian Joint) *The coordination of information effects to influence the decision making and actions of a target audience and to protect and enhance our decision making and actions in support of national interests’.*

A second issue with the term information operations is that it is somewhat at odds with other Australian Army doctrinal guidance and recommended ABCA standards. At present,

the term “operation” is used openly, with a wide range of Actions described as operations. Examples are “bridging operations,” and “transport operations.” The reference aims to establish tighter usage and more precise meaning within a defined spectrum. For example, the Australian Government’s commitment to stability in the Solomon Islands, Operation Anode, conducts four types of activities: offensive, defensive, stability, and enabling. Enabling activities can be described as tactical actions that link, support, or create the conditions for offensive, defensive, and stability activities.

Offensive activities in turn have a number of associated actions, such as: attack, advance, and pursuit. Within an offensive activity (including defensive, stability, and enabling activities), information actions would be intrinsically organic to the conduct of that activity, and may be represented in one or more (simultaneous or separate) information actions. We can use a number of tools to best effect implementation of the information action (Figure 1).

The Australian Army is therefore considering replacing the term information operations with *information actions*. An emerging Australian Army definition under consideration is:

Actions conducted to influence target audiences in order to achieve understanding, acceptance, and support of our actions and aims, and to diminish the quality and speed of the adversary’s decision making, while maintaining our own, to achieve decision superiority.

Battlespace Operating System

In the Australian Army tactical lexicon, information operations is also referred to as a battlespace operating system (BOS). This is a framework within which a force synchronizes actions across the battlespace. The Army further envisions moving away from the title of ‘IO BOS.’ Accordingly, they are considering a number of titles, including ‘information dominance and influence’ (IDI) BOS. This reflects an Australian Army view that the previously-titled BOS needs to reflect information dominance in terms of effective electromagnetic environment management—resulting in domination of adversary or neutral information and protection of one’s own. Additionally, core influence activities are incorporated into the BOS, extending not only across the information environment, but also the cognitive environment of any target audience.

Core Components of IA

At present, information actions are the integrated employment of a number of core capabilities: deception, psychological operations (PSYOP), electronic warfare (EW), operations security (OPSEC), and computer network operations (CNO). Additionally, IA has a number of supporting capabilities, including physical attack, information security, and some related capabilities—public information and civil-military cooperation (CIMIC). These various capabilities can be employed across three core information actions that align to the broad ABCA working group’s recommendations. The core actions are:

| Title | Activity | | Actions | Info Actions | Capabilities/Tools |
|---|------------------|----------------------------|----------------------------------|--|---|
| A Military Operation, eg OPERATION ANODE | Offensive | Information Actions | Attack, Advance, Pursue, etc. | 1) Influence 2) Counter Command, 3) Command & Info Protection | PSYOP, MILDEC, EW, CNO, CIMIC, PI, MPA, PPP, OPSEC, HUMINT, Targeting, (Example list) |
| | Defensive | | Static, Delaying, Mobile | As above | As above |
| | Stability | | etc. | As above | As above |
| | Enabling | | etc. | As above | As Above |

Figure 1. Link between an Operation, Activity, Action, and Capability in Describing Information Actions.

1. Influence: aimed at changing the perceptions and will of target audiences.

2. Counter Command: focused on diminishing the adversary's command and control systems and associated decision making.

3. Information and Command Protection: focused on protecting our own information and command and control and information systems.

Influence actions include employing the supporting capabilities of Military Public Information, PSYOP, deception, CIMIC, plus presence, posture, and profile tasks. However, depending on the results of ongoing analysis, this list may eventually include other tactical capabilities.

Counter command actions include employment of a range of capabilities or tools. OPSEC, EW (specifically electronic attack), and CNO (computer network operations, including attack) are predominantly focused on the physical dimension of information terrain (information systems). Deception and PSYOP focus on the cognitive dimension (decision makers' brains). Yet we may also employ other capabilities enabling physical destruction of enemy commanders, their staffs, and systems. Coalition staffs would draw on the assistance and advice of specialist staff areas such as EW, PSYOP, and kinetic targeting as appropriate. The Australian Army is still analyzing which staff function should have responsibility for Counter Command Activity.

Information and command protection actions include employment of a range of capabilities including information security, EW (via electronic protection), CNO (primarily, computer network defense), OPSEC, counter deception, and counter PSYOP/counter propaganda. While information and command protection actions would most likely draw heavily on the assistance and advice of specialist staffs, indications are that "operations" or the "3" may be the most appropriate responsible staff area. Notably, the ABCA Armies' draft report refers to this activity solely as information protection, though the Australian Army is still examining inclusion of command protection. There is an obvious need to address protection of our own commanders, staffs, and command and control systems against the adversaries' counter command activity.

Furthermore, commanders are increasingly likely to encounter a range of actions intended to impair or diminish the quality of their decision making, and their ability to command effectively. With our increasing IT reliance, modern armies

and commanders will undoubtedly face hostile activity directed towards destroying or impairing automated command and control and information systems.

Defense against such measures is the core information and command protection activity. Physically, commanders, their headquarters, and staffs could be subject to destruction by a range of weapon systems or attacks. Defense against such hostile actions is the realm of OPSEC, as well as defensive force protection and other security measures. Commanders may be the target of deception measures, or PSYOP intended to impair the quality of their decisionmaking. Defense against such measures is achieved through effective intelligence, surveillance, target acquisition, and reconnaissance (ISTAR), enabling accurate situational awareness, understanding, and counter deception measures.

The potential for all service members to be subject to an evolving class of incapacitating or debilitating weapons is also increasing. The following quote advocates the need to "firewall" the minds of commanders, staffs, and systems operators:

We are on the threshold of an era in which these data processors of the human body may be manipulated or debilitated. An entirely new arsenal of weapons, based on devices designed to introduce subliminal messages or to alter the body's psychological or data processing capabilities, might be used to incapacitate individuals.

We are potentially the biggest victims of information warfare, because we have neglected to protect ourselves.

Our obsession with a 'system of systems' is most likely a leading cause of why we neglect the human factor in our information warfare theories. It is time to change our terminology and our conceptual paradigm. Our terminology confuses us, sending us in directions dealing primarily with hardware, software, and communications components. We need to spend more time researching how to protect the *humans* in our data management structures. We cannot sustain anything within those structures if we're debilitated by our adversaries. Right now someone may be designing the means to disrupt the human component of our carefully constructed notion of a system of systems.

There has been significant development in the evolution of mind- altering weapons since the preceding quotes were written. While much more than a doctrinal issue, there is obvious value in placing greater emphasis on protection of

commanders, their staffs, and systems operators. Hence, the Australian Army is considering inclusion of “command” into the core activity of information and command protection.

Information Actions and Intelligence Preparation of the Battlespace

Australian Army planning doctrine includes a chapter on Intelligence Preparation of the Battlespace (IPB). The description places more emphasis on factors that have far wider scope than the traditional domains such as physical terrain, weather, conventional or adversary weapon capabilities, and tactics, techniques, and procedures. These factors include: the electromagnetic spectrum, societal, political, cultural, religious, and economic aspects, with this list not being exhaustive. Past Australian Army doctrine gives limited consideration of information terrain and human terrain; future doctrine will address these areas in more depth.

The information terrain is an increasingly important component of the battlespace. It includes the individuals, organizations, and systems of both friendly and adversary forces that collect, process, or disseminate information—as well as the information itself. It also includes the civilian population and governmental agencies that coordinate international efforts, non-governmental organizations, and the news media. Accordingly, the information terrain and human terrain are interconnected.

Australian Army doctrine regarding information actions needs to address intelligence support, through the IPB, to all core areas of information actions. Given recent operational feedback and associated criticisms of current doctrine, we should place more emphasis on intelligence support to influence, particularly in respect to peace support and counterinsurgency operations. Much greater emphasis could be placed on defining, describing, and understanding the diverse groups and micro populations that may exist in an area of operations and areas of interest. For each segment of the population, as well as the overall population, this would include aspects such as aspirations, motivations, goals, religions, leaders, leadership rivalries and associated factions, alliances, loyalties, obligations, hatreds, daily rituals, historical dates and cultural norms.

Likewise, the Australian Army is considering information actions, its roles, and relationships across the five lines of operation considered within adaptive campaigning:

1. Joint Land Combat - Involves actions to secure the environment, remove organized resistance, and set conditions for the other lines of operation;
2. Population Protection - Provides protection and security to threatened populations in order to set the conditions for the re-establishment of law and order;
3. Public Information - Informs and shapes the perceptions, attitudes, behavior, and understanding of target population groups;
4. Population Support - Establishes/restores or temporarily replaces the necessary essential services in effected communities;



*Commonwealth of Australia
(Univ. of Texas)*

5. Indigenous Capacity Building - Nurtures establishment of civilian governance (local and central), security, police, legal, financial, and administrative systems.

Based on contemporary operational experience, there appears to be a growing recognition that Australia should adopt a broader, more comprehensive, yet more systematic approach to information-related actions. The answer to current difficulties in applying information actions to operations is not to abandon the concept, but to “think outside the box” and improve on it.

In order for this to occur, the Australian Army is currently developing doctrine to meet the needs of the tactical commander. This will further develop concepts discussed in this article, to ensure that information actions broadly align to the Australian joint IO approach, and help the Army implement its components of any or strategic shaping and influencing plan. Additionally, the Australian Army is cognizant of the ABCA Program’s works, and of the need for doctrinal interoperability with other nations.

Development of Australian Army doctrine will enable refinement of information actions and capabilities, by providing guidance to commanders and their staffs on the most effective employment of IA-related capabilities across the IDI BOS. Underpinning this development is that information actions are intrinsically one of the four types of activities: offensive, defensive, stability, and enabling. Accordingly, we must plan information actions in conjunction with all aspects of a military operation, to ensure success and relevance in the future complex operating environment —across all lines of operation.

Defeat or Neutralize Extremists’ Use of the Internet?

How Australia plans to defeat or neutralize extremist use of the Internet raises a number of issues. First and foremost are those actions undertaken by a ‘Whole of Government’

approach: employing strategic, operational, and tactical capabilities that revolve around management and domination of the electromagnetic spectrum. Yet we must examine other issues relating to extremist Internet use: spectrum of interest; scenario generation; countering extremist Internet-based influence actions; risk mitigation; and national policy considerations.

Spectrum of Interest

First, it is important to look further afield than just the extremist group. We must also acknowledge that an extremist group attempts to influence an audience. This may range from a domestic population (with its various sub-groups), where military or stabilization operations are being conducted; to the domestic audience (including political) of the contributing coalition nations. More broadly, we must consider a world audience who may or may not be sympathetic (depending on country, background, and/or culture) to the extremists' cause. The latter audiences will hold ongoing interest in both what is occurring, and what is being released via Internet and other media. This may be due to personal connections to the events as they unfold, a cultural or socio-economic link, or a base level interest centered simply on curiosity.

While adversary use of the Internet will continue and expand, it is how coalition nations discredit adversary themes and messages across the majority of audiences described, that make adversarial Web influence actions redundant. Thus, the remainder of this article examines how adversaries seek to gain influence, versus dominate the electromagnetic spectrum from a technical perspective.

Adversaries look to exploit the broad fringe populations within the spectrum of interest. In simple terms the adversary seeks to: separate and splinter local populations against occupying forces or agencies, or for those groups that are neutral to the adversary and the coalition; or subvert them to provide full support by joining in adversary activities. Subversion could be achieved via the provision of finance, weapons, safe houses, or more simply just not providing information to an occupying force on known or intended adversary activities. Additionally, extremists will target contributing coalition nations' troops and commanders, in an attempt to affect morale and the overall success of the military operation.

Noting the extremists' spectrum of relative interests, it is likely the same spectrum would apply to any coalition conducting IO (Figure 2). In this author's opinion, what makes coalition IO slow to counter extremist Internet use is not an issue of technological superiority, nor lack of ability to respond—but inflexible command structures that do not enable quick and effective counter-computer network ops. This is especially pertinent for audiences in the “friendly but uncommitted,” “neutral,” or “inactive hostile” range of influence.

Scenario Generation

An example of how extremists use information is reflected in the following scenario:

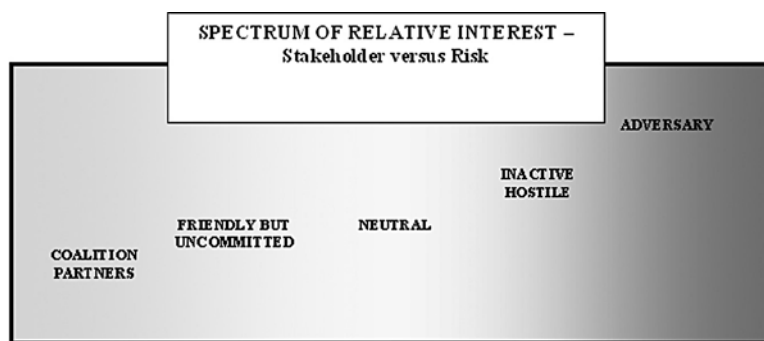


Figure 2. Spectrum of Interest.

- Extremists react to the outcomes of a coalition tactical action by posting either staged, incomplete, or deliberately incorrect website transmissions, to gain maximum effect on one or more groups outlined in the spectrum of interest;
- Coalition reaction (based on the ability to effectively upload accurate combat camera images or other imagery), devises a response at the tactical IO level in the area of operations;
- A coalition response would require operational level approval, from those who vet—and if required—recommend changes to any proposal. Additionally, forces may request further guidance from experts at the military-strategic decision-making level, with the possibility of input from non-military strategic decision-makers and bureaucrats;
- Concurrently (and noting the known delays imposed by command and control), extremists are planning to launch the next information Web activity aimed at influencing those populations within the spectrum of interest. One could interpret that extremists' second and third order Internet influence activities (possibly without a friendly counter-influence activity targeting the first extremist Internet action) are inside the response cycle of a coalition or a single nation;
- Accordingly, extremists can and will continue to force coalition reactions to their Internet activity. In this scenario, extremists identify and target the coalition's critical vulnerability of being unable to implement rapid response to Web-based information actions.

Countering Extremist Internet Based Influence Actions

To counter extremist dominance, in terms of uploading their IO messages and disseminating a message quickly to achieve influence, coalition individuals/groups who conduct tactical level IO need to be empowered. Leaders at brigade level and below must be able to make command decisions about the responses they devise, and to launch rapid counter network-based influence actions.

This in conjunction with robust implementation of a Military Public Information plan that supports and highlights coalition strengths, sending messages to the world's media and domestic populations that compliment coalition Internet actions. Concurrently, PSYOP and CIMIC would look to build on the influence that “neutral” or “inactive hostile” audiences are exposed to via coalition Internet actions.

Risk Mitigation

An associated risk of empowering the tactical IO commander is that the tactical IO message may not exactly mirror the military-strategic IO message. We can mitigate this risk by effective and direct communication between the IO command levels, enabling a detailed understanding of the strategic shaping and influencing (S&I) plan established by a “Whole of Government” approach. Thorough understanding of the S&I plan, in addition to robust comprehension of the operational and tactical IO themes and messages, will assist in risk mitigation and ensure timely and appropriate responses.

While the outcome of the proposed solution enables a quick response, some could still probably view it as reactive. However, it does have a second order effect of making the coalition operational/tactical IO staff less encumbered by time intensive staffing issues—and more empowered by proactive information Internet actions. Once implemented, such actions would force an extremist group to consider an influence response. Accordingly, the extremists’ ability of to get inside the coalition’s Web-based influence decision response cycle starts to erode, forcing the extremists to respond to out influence activities.

While an extremist group may choose not to respond with counter Web-based influence activities, it is at this stage (acknowledging that technical attacks are a separate critical target for extremists), that a coalition starts to achieve Web-based decision superiority. While this approach may not completely negate extremist use of the Internet, combined with technological domination of the electromagnetic spectrum, it will make extremists’ Web-based influence actions more difficult.


National Policy Considerations

Achieving influence “action-decision” superiority across the spectrum of influence enables a coalition to consider implementing more aggressive targeting of extremists. Web-based information deception is but one example. To enable effective information deception, national governments must consider Internet-based rules of engagement that empower the tactical commander to launch information deception against Web-based extremists. While this is a delicate legal and ethical subject, in terms of how different nations empower their forces, we must acknowledge that extremists operate under no such restraints. They are essentially free to conduct Internet-based influence actions as they desire.

Extremists retain the ability to utilize the Internet for influence activity, knowing that a coalition is only able to conduct counter-actions that adhere to restrictive rules of engagement. Future examination of national policies and procedures (at a military-strategic and political-

strategic level), are needed in order for coalition Web-based influence actions to encounter less operational hindrance. We could continue to hear comments such as “we are failing to win influence and are being defeated by technologically competent extremists in the area of influencing perceptions,” unless there is a unified will to empower coalitions to conduct influence operations free of encumbrances. Such freedom of action still needs to maintain the moral and ethical high ground, and be appropriately balanced. Yet it demands a tactical and operational freedom of action which allows degradation of extremist influence operations on the Internet. Accordingly, national governments need to empower the highest-level military-strategic decision-makers and strategic and operational commanders to authorize responsive, appropriate tactical-level actions.

From a non-technical perspective, preemptive or pro-active dislocation of extremist Internet presence is best achieved by implementing an aggressive IO campaign which saturates the Internet with favorable messages. This should create a situation where extremists, in order to pursue their own IO Internet agenda, are forced to react to an overwhelming coalition Internet influence campaign. Otherwise, extremists have an open time frame within which they can initiate unhindered support for their influence campaign.

Combined with technological domination of the electromagnetic spectrum, reflections presented here are just some of what we need to further explore. In order to combat extremist use of the Internet, we must degrade their ability to dominate influence activities. We must keep them from reaching audiences within the spectrum of interest. 

is a